International Journal of Future Generation Communication and Networking
Vol. 13, No. 3s, (2020), pp. 103–109

Network Security Enabled Arduino Devices for Military Communication

Kasturi Shet[1], Neha Shilamkar[2], Pradnya Kamble[3], Harsh Choudhary[4], Pooja Vengurlekar[5]

Computer Department, Savitri Phule Pune University

[1]kasturishet5@gmail.com

[2]nehashilamkar@gmail.com

[3]kamblepradnya02@gmail.com

[4]102harsh301@gmail.com

[5]pooja.v.85@gmail.com

Abstract

Today, India's primary mission is to detect and prevent the entry of terrorists, weapons of mass destruction, and illegal allies. Indian army has a long and storied history as our nation's first line of defense against unauthorized access of terrorists into the country, and to interdict drug smugglers and other criminals along the border. Thus, military men need highly secured communication device having encryption decryption technology and password protection. This system must be non-hackable and it must provide secured communication between soldiers at border. The sole purpose of this system is to establish the communication between two soldiers. We will be using two Arduino devices with 32-bit SSL encryption and communication between two devices is established by Zigbee protocol which is 128bit AES encryption. Hence double encryption will be achieved. Serverless point to point communication cannot be hacked as data is not stored at any physical location.

Keywords— Military Communication, Security, Network, Zigbee.

I. INTRODUCTION

Migration and terrorist attacks are the top most crucial issues today. Today, the India's primary mission is to detect and prevent the entry of terrorists, weapons of mass destruction, and illegal allies in the country. India has a long and storied history as our nation's first line of defence against unauthorized forces into the country, and to interdict drug smugglers and other criminals along the border. Hence, military men need highly secured communication having encryption and password protection. This system must be non-hackable and should provide security while communicating. The purpose of this system is to establish a secure communication between two soldiers. India's most concerning issue today is terrorism and maintaining highest possible security at the borders. It is extremely essential to provide highly secured communication model to the military men. Any sort of message leakages, unauthorized access of data and frequency hacking can directly allow access to the private messages and missions of the armed forces to enemies. Today's communication model used by our military men is walkie-talkie. This works on frequency transmission for message passing. As through various techniques this frequency (in some cases) can be hacked, a more secured communication model is necessary that will doubly encrypt the message and thus any kind of leaks can be avoided.

ISSN: 2233-7857 IJFGCN

II. LITERATURE REVIEW

Than Myo Zaw et.all [1] proposed the idea of securing SSL protocol with zero-knowledge proof, which is essentially a user authentication. The scheme is combined with zero-knowledge for certificate, which is directly transfer from server to client and client to server. Not only sever but also client have certificates that they want to prove to each other, but they don't want to tell the secret (certificate) itself to each other. Client ask server also server asks client a series of questions, trying to find out if client and server really have the secret (certificate) or not. Client and server do not learn anything of the secret (certificate) itself, even if they would cheat or not adhere to the protocol. If they were to repeat this trick many times, say 20 times in a row, their chance of successfully anticipating all of their requests would become vanishingly small (about one in a million). Finally, SSL used in Handshake protocol with Zero-Knowledge Proof proposed for an intruder should not be able to substitute false certificates and masquerade as client or sever.

V. A. Desnitsky et.all [2] aim at researching the subject area, models and prototypes of secure mobile communication mesh networks providing support and operational management in critical emergency situations. Such a network represents a command technical complex that provides services of text messages and media data transfer, database services, web services, etc. A two-layer network architecture using Arduino microcontrollers and XBee Series 2 modules, implementing business processes and wireless communications by ZigBee protocol is proposed. The two-layer character of the network allows organizing isolation of data flows between particular subnets, nodes and users effectively.

Khamar Ali Shaikh [3] explains the main objective of the Secure Socket Layer (SSL) which is to build secure data transactions between two applications. It is made up of two layers. It is layered on the top of some reliable protocol layer like TCP. The SSL record convention helps in encapsulating the higher-level protocols. One such encapsulated protocol, the SSL handshake convention helps the server and the client to verify each other and to follow an encryption method to produce cryptographic keys before the application data is being transmitted over the network. Thus, the data can be read only by the authenticated client. Great advantage of SSL is that it is application protocol independent. Application data messages are encrypted using the previously decided encryption method and generated master key for symmetric encryption. Secure Socket Layer is widely used to secure the information transaction and to prevent the attacks, Transport Layer Security (TLS) is being preferred due to its numerous vulnerabilities in it.

Julham.et all [4], present that Arduino is an open source electronic circuit board that uses a microcontroller ATmega328P-PU. The Arduino type used was Arduino Uno and the encryption technique was substitution. The substitution encryption technique was applied for data communication security between Arduino Uno worked well. Substitution encryption application in Arduino Uno can be used in asynchronous serial communication. The second testing requires the modification of data received from sensor, especially for single digit data to be double digit data. Creating encryption and decryption keys in Arduino Uno should be the same.

Ievgeniia kuzminykh.et all [5], focus on ZigBee wireless technology and testing ZigBee end devices in order to see how transmission range impacts on quality parameters. Since only a small amount of data typically must be transmitted between these connected devices, reliable, cost-effective wireless communication protocol like ZigBee is ideal. ZigBee Remote Control

ISSN: 2233-7857 IJFGCN

protocol has few significant advantages among systems offering low-power transmission, robustness, high security and high scalability with high node density and it also takes n advantage of wireless control and sensor networks. In this paper the configuration and testing of ZigBee modules was preformed through the use of the software X-CTU.

Vivek Negi et.all [6] theorized that the security in terms of Networks have turned out to be more significant to Organizations, Military and personal computer users. Since various kinds of threats are there for data sent from sender side over internet till it reaches to receiver. It transform our data into unintelligible form, data which will be sent can be text or no text form, by encrypting the data and we can save it from attacks like eavesdropping, in which interception of communication by unauthorized person, he can either listen or can add malicious information in our data which can lead to catastrophic results. This technique of securing data transmission is very useful in securing the integrity of data sent by the Unmanned Aerial Vehicles in military application to commercially used Electricity meter. Since the above mentioned devices uses microcontroller to send data through internet hence this data is always going to be susceptible to above mentioned threats so it is important to ensure that it doesn't fall in wrong hands, our objective is that our microcontroller sends the data to remote location has authenticity, confidentiality and integrity.

Akmal Nurhananie Abd Rahman.et all [7], in this paper author presents the application development conducted for Android devices and the current results achieved. The project focused on using ZigBee-based technology. The development of mobile platforms is very rapid and significant lately, especially for Android, where it is even faster than the development of hardware devices that enables the new data applications. Peer-to-Peer (P2P) is a very popular type of network communication for file sharing, where the data transfer is faster as it does not need to pass through the services of a server to share files and data. For the time being, the successful P2P applications have been running on either the wired or wireless Internet connection, as well as over PAN network such as Bluetooth.

Yao-Nan Lien et.all [8] discussed an idea about the safety and security driven approach to embedded system design for an Industrial class of internet-based applications. It discusses an integrated networking framework stemming from the IEEE 1451.1 smart transducer interface standard, which is an object-based networking model supporting client-server and publish-subscribe communication patterns in group messaging, and from the IP multicast communication, all together mediating safe and secure access to smart sensors through Internet. ZigBee protocol and IEEE 1451 concepts are used for its low – powered wireless networks specifications.

Miroslav Sveda et.all [9] suggested that the design of subsystem of P2Pnet, a Walkie-Talkie-like communication system, which can be used in the early hours or days after a natural disaster strike. We wish to stimulate the research on the emergency communication systems that is inexpensive and easy to deploy for future catastrophic natural disasters. The most important lessons we learned from numerous disasters are that mobile communication systems are very vulnerable and the loss of communication system may have a catastrophic consequence. Also, the design of a Walkie-Talkie-like communication system over a MANET based P2Pnet.

Majed Abu Khater et.all [10] summarizes about unprotected communication over a normal network is quite risky. Today, especially with the widespread abuse of electronic communication

ISSN: 2233-7857 IJFGCN

through eavesdropping and viruses. This presents a challenge in an environment where remote monitoring of equipment is required. Especially if the operation is of sensitive nature or the equipment is based on proprietary IP. We have shown that DES is well suited for such implementation in part to its low computational complexity and small memory footprint. Both of these features enable the implementation of very low-cost systems that would not affect the margins or bottom line of the embedded system. DES presents a compelling argument for securing the communication in all embedded systems. However, one must always remember that there is no fail-safe encryption system and the strength of such a system is as strong as its weakest link. For DES that would be the safe-keeping of the secret key.

III.METHODOLOGY

The proposed system has two users' sender and receiver. The sender system consists of an android device with an android application installed on it, a Bluetooth to receive messages from the android device, a ZigBee module to transmit the received message to the receiver side, a microcontroller and an Arduino board to install all the components. The microcontroller is an Atmel 8-bit AVR RISC-based microcontroller combining 32 KB ISP flash memory with read-while-write capabilities, 1 KB EEPROM, 2 KB SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented 2-wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channels in TQFP and QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts. The device achieves throughput approaching 1 MIPS per MHz

As shown in Fig.1 (a) when the sender opens the application, a timer of 5 minutes gets started in the background, which when detects inactivity of five minutes logs out the application. Also, the application is password protected. If wrong password is inserted more than 3 times it automatically stops the functioning of the device. After login successfully sender has two options either to type the message or there is a speech to text recognition API installed on the application which can convert the speech to text. Now the message gets transferred to the Arduino board which is connected to android device via Bluetooth. The message sent from android device to Arduino device gets 8-bit SSL encrypted. Which further gets passed to the receiver's end via Zigbee which has 128bit AES encryption.

As shown in Fig.1(b), when the message is received by the receiver Zigbee, it gets 128-bit AES encrypted which is further decrypted by the Zigbee module and then the message gets forwarded to the android application via Bluetooth where in again a decryption of 8 Bit SSL is done. Now the message has finally reached the receiver. To view the message the receiver needs to log in the device which is password protected.

ISSN: 2233-7857 IJFGCN

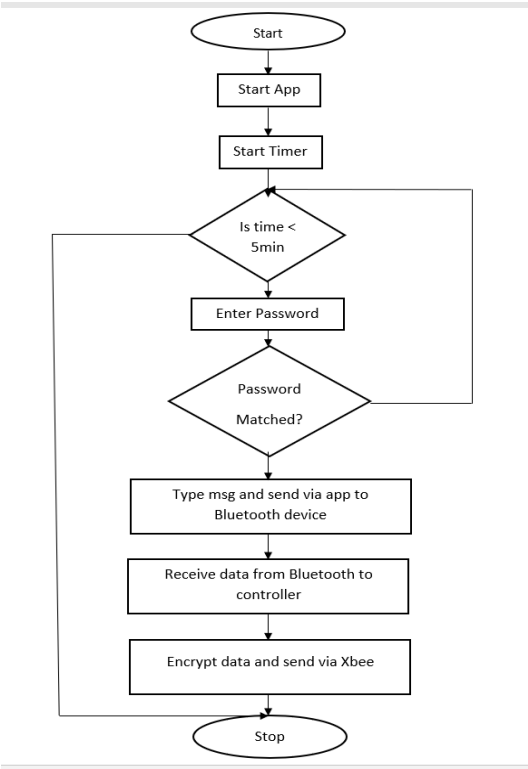

Fig. 1(a) Flow Chart (Sender)

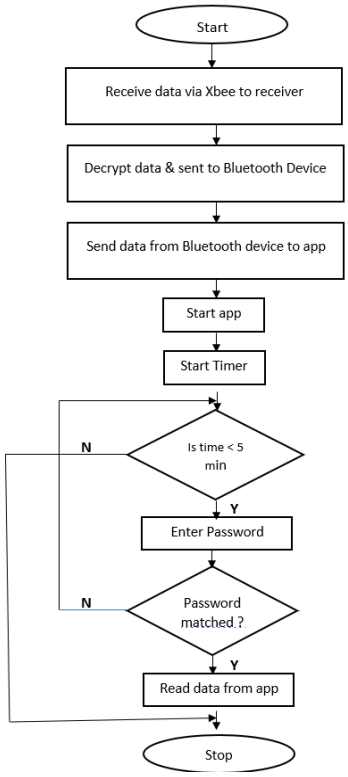

Fig. 1(b) Flow Chart (Receiver)

IV. SYSTEM ARCHITECTURE

As shown in Fig 3, system architecture has two Arduino Microcontrollers having with SSL for encryption-decryption and Zigbee for communication between two Arduino devices, Keypad for typing the message and LCD (Liquid Crystal Display) for displaying the message are connected to microcontroller and lastly android device is connected via Bluetooth to Arduino board. This device contains android application through which one can send or receive the message.

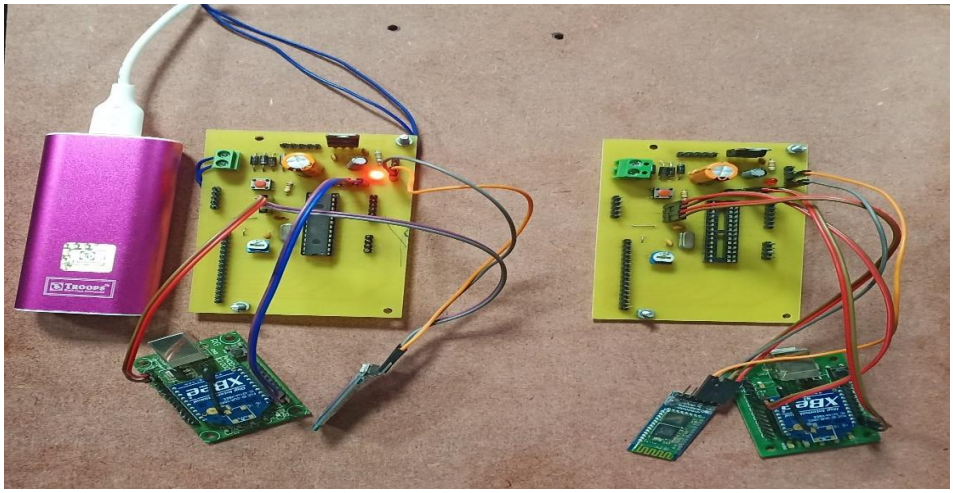

Fig. 2 Hardware

ISSN: 2233-7857 IJFGCN

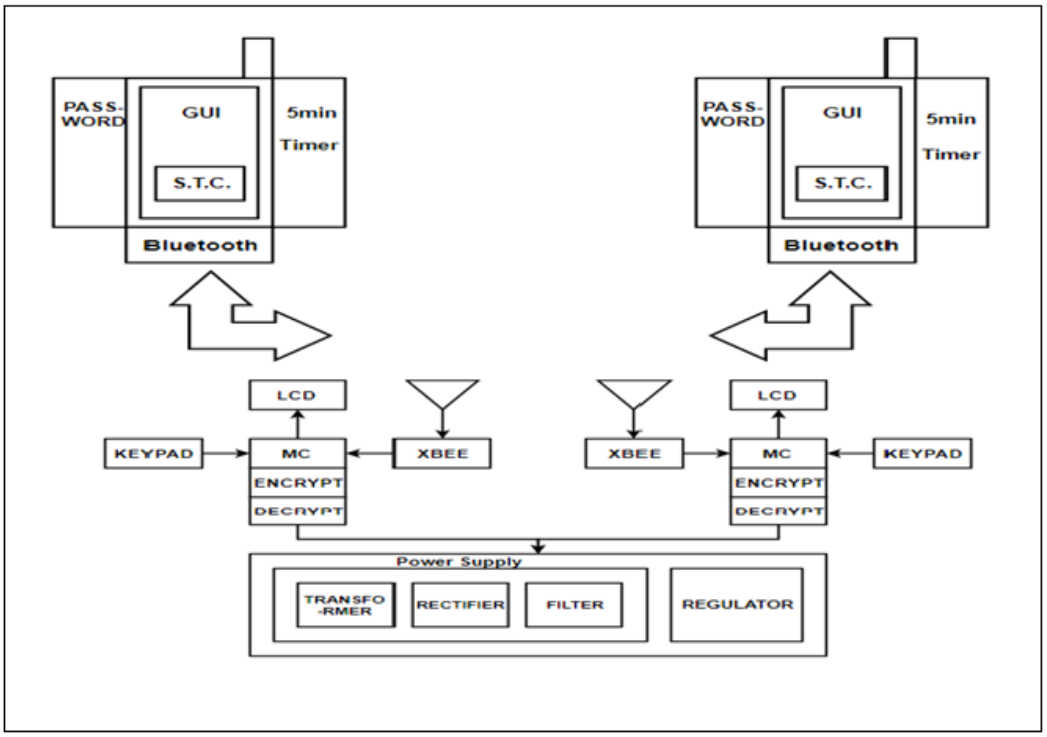

Fig. 3 System Architecture

As soon as the sender will send the message using his/her android application, it will get encrypted via SSL and this encrypted message will be passed to the microcontroller and will again get encrypted via Zigbee once the message has been received from the microcontroller to the senders ZigBee module. In this way double encryption is achieved. On receiver side same process will be followed in descending manner and once the message gets decrypted receiver can view the message.

V. Result and Discussion

This system is developed to establish an encrypted and secured communication system in areas of less connectivity and no internet like country borders. Communication between devices is established using Zigbee which can have a range from 100m to 64km depending on the Xbee module we use. System consists of a sender device, a receiver device and a mobile application that needs to be installed on both sender's and receiver's mobile phone. Sender needs to login the device with his unique password, 5 continuous failed attempts to login will result in permanent broken connection between mobile and the device. After successful login message sent by sender reaches sender device via Bluetooth with 128bit SSL encryption, device needs to be in the Bluetooth range for message to transmit from mobile to device, so preferably it can be kept in pocket or bag of soldier. This encrypted message is again encrypted by 128 bit AES encryption and also by a unique encryption technique developed by us. Now this encrypted message is sent using Zigbee module. Zigbee has digital signals which is difficult to intercept in between. Once message reaches The receiver device, process of deception starts in the reverse manner on encryption and then the message is forwarded to the receiver's mobile, which he needs to login to view the message. Message automatically gets deleted after 5 minutes once it's seen.

ISSN: 2233-7857 IJFGCN

VI. CONCLUSION

This paper puts forward a system that provides highly secured communication between two authorities. With enhanced digital security level and integration of embedded system the system encryption keys will be non-hackable and highly secured. Hence, the system will provide double encryption firstly with SSL and secondly with Zigbee.

VII. FUTURE SCOPE

The scope of current system can be increased from point to point communication to broadcast. Thus, large network of communication can be implemented for more than two people. System can be upgraded with long range facility and encryption level increases by using double encryption. This can be achieved by using higher range of Zigbee module.

REFERENCES

[1] Than Myo Zaw, Min Thant, S. V. Bezzateev "User Authentication in SSL Handshake Protocol with Zero-Knowledge Proof", Saint-Petersburg State University of Aerospace Instrumentation Saint-Petersburg, Russia, 2018.
[2] V. Kotenko, V. A. Desnitsky, "Modeling and Analysis of Security Incidents for Mobile Communication Mesh Zigbee-Based Network", 978-1-5386-1810-3/17/, 2017.
[3] Khamar Ali Shaikh, Karthik Bhat A, Minal Moharir, "A survey on SSL packet structure",Student Computer Science and Engineering Department , RVCE, Bengaluru, Karnataka, India,2017.
[4] Julham, Ferry Fachrizal, "Security of Data Communications Between Embedded Arduino Systems with Substitution Encryption", Computer and Information Engineering Politeknik Negeri Medan Medan, Indonesia, 2017.
[5] Ievgeniia Kuzminykh, Arkadii Snihurov, Anders Carlsson, "Testing of Communication Range in ZigBee Technology", Telecommunication Systems Dept., Kharkiv National University of Radio Electronics, UKRAINE, 2017.
[6] Vivek Negi, Himanshu Verma, Ipsita Singh, Adity Vikram, Kanika Malik, Archana Singh, Gaurav Verma, "Network Security in Embedded System Using TLS",Department of Electronics and Communication, Jaypee University, A-10, Sector-62, Noida (U.P.), India,2016.
[7] Akmal Nurhananie Abd Rahman, Mohamed Hadi Habaebi, Mahamod Ismail, "Android-based P2P File Sharing Over ZigBee Radios" Electrical and Computer Engineering Department International Islamic University Malaysia, Kuala Lumpur, Selangor, 2014.
[8] Yao-Nan Lien, Li-Cheng Chi, and Yuh-Sheng Shaw, "A Walkie Talkie-Like Emergency Communication System for Catastrophic Natural Disasters", Dept. of Computer Science, National Chenchi University, 2009.
[9] Miroslav Sveda and Roman Trchalik, "Safety and Security-driven Design of Networked Embedded Systems", Brno University of Technology Bozetechova 2, CZ-612 66 Brno, Czech Republic, 2007.
[10] Majed Abu Khater, Malek H. Amro, Anas Abu Laban, Bassel Soudan, "Secure Communication in an Embedded Environment",Department of Electrical and Computer Engineering University of Sharjah, 2006.

ISSN: 2233-7857 IJFGCN